IDA

INSTITUTE FOR DEFENSE ANALYSES

Exploratory Analysis of Supply Chains in the Defense Industrial Base

James R. Dominy, Project Leader
Scot A. Arnold
Forrest R. Frank
Jenny R. Holzer
James N. Richmann

April 2012

IDA Document D-4308
Log: H 11-001593

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About this Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract DASW01-04-C-0003, AH-7-3315, "Exploratory Analysis of Supply Chains in the Defense Industrial Base," for the Director, Industrial Policy. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Thomas P. Frazier, David E. Hunter, and Marius S. Vassiliou were the technical reviewers for this document.

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-4308

Exploratory Analysis of Supply Chains in the Defense Industrial Base

James R. Dominy, Project Leader
Scot A. Arnold
Forrest R. Frank
Jenny R. Holzer
James N. Richmann

Executive Summary

Introduction

The Institute for Defense Analyses (IDA) was tasked by the Deputy Assistant Secretary of Defense (Manufacturing and Industrial Base Policy) to perform an exploratory analysis of the supply chains for the Unmanned Aerial Systems (UASs) and Cyber Security Equipment and Services sectors of the Defense Industrial Base as part of its Sector-by-Sector, Tier-by-Tier initiative. Specifically, for these two sectors, IDA was asked to identify:

- Segments of the supply chain that depend on a sole supplier or on constrained competition;
- Interdependencies across programs or across prime contractors' supplier networks;
- Companies that possess major capabilities for design of future products in the sectors;
- The relationship between the military and commercial markets in each sector, including variation across sub-tiers within each sector;
- The degree to which the supply chain is global in nature; and
- How key companies get access to working and investment capital at the various tiers of the supply chain.

Our main findings are summarized below.

Unmanned Aerial Systems (UASs)

Since the UAS is a relatively new technology, the industry is still in a maturing stage. The United States is the world leader in UAS acquisition and use, and U.S. firms have over two-thirds of the overall market. Our review identified 125 U.S. producers and developers of UASs, ranging from large Department of Defense (DoD) prime contractors to research laboratories and small firms trying to break into the market. Our review also identified 50 U.S. companies producing UAS payloads, 25 U.S. suppliers of UAS engines, and 25 U.S. UAS avionics manufacturers. Most of the materials and subsystems are not unique to the UAS sector but are leveraged from manned military or general aviation. Data links (such as the Tactical Common Data Link (TCDL)) and ground control stations are examples of components developed specifically for UASs.

Issues of Sole Supplier or Constrained Competition

Although we did not identify any sole-source supplier constraints at the system level, we note that few U.S. companies (such as Northrop Grumman (NG) and General Atomics) possess the infrastructure and expertise to produce large UAS platforms. These firms also dominate the large UAS service industries. Likewise, only a few companies serve as prime contractors for UAS sensor systems. We find, however, that as the large prime contractors focus their efforts more on system integration, opportunities for small and medium-sized second-tier manufacturers become available.

We do find examples of constrained domestic competition at the component and materials levels. We also found that, because DoD UAS programs rely heavily on commercial components, Diminishing Manufacturing Sources (DMS) can constitute a major supply chain problem as the original components cease to be available in the commercial marketplace. As an example, NG estimates that at least 700 components of the Global Hawk system are affected by DMS.

Interdependencies across Programs or Prime Contractors' Supplier Networks

The DoD is currently attempting to standardize elements of UASs, which, in turn, will create interdependencies across programs. For example, the TCDL is the current standard for larger UASs for secure delivery of data to ground stations and is currently built by multiple contractors. The Air Force is attempting to standardize secure data links for small (<30-lb) UASs. Although this design will be non-proprietary and government owned, it might create an issue for new, small UAS developers attempting to break into the market since the firm will have to have a government contract to qualify for this government-furnished equipment (GFE) data link. The Services are also attempting to standardize their ground control stations.

Standardization of data links and ground control stations can be expected to create interdependencies across programs. However, due to security issues, these components are currently made by a very small number of U.S. manufacturers. In this case, the government may potentially be creating an expensive sole source. For other components, for which the particular manufacturer is not constrained by security concerns, standardization may have an alternative consequence. Here, standardization may serve to increase the quantity of the item to be procured, thus creating sufficient demand to attract additional firms to bid on future procurements.

Companies with Major Capabilities for Design of Future Products

Our research leads us to conclude that innovation in enabling technologies in the UAS market comes primarily from smaller firms. Larger firms are buying these smaller firms to enter or expand their share of particular market segments; however, this strategy

then carries the potential risk that innovation may be impeded as the design teams for these programs migrate from small firms to large firms.

AeroVironment is an example of a small ($250 million in sales) company that is currently one of the largest players in the small Unmanned Aerial Vehicle (UAV) market. They are currently engaged in research in several new platforms: the Global Observer, which is a high-altitude, long-endurance UAV, and the Nano Air Vehicle, which is a Defense Advanced Research Projects Agency (DARPA)-sponsored program to develop a 10-g UAS that can hover for extended periods. Academic research is also pushing the technology envelope in nano- and pico-scale UASs.

Relationship between Military and Commercial Markets

At present, there is not a broad civil or commercial market for UASs since they are not able to routinely access the U.S. airspace system. When airspace control procedures for control of UASs are in place, the market can be expected to expand significantly. At the subsystem/subcontractor level, however, there is a significant relationship between the commercial and defense UAS markets. In addition, small and man-portable UASs use small displacement internal combustion engines or electric motors that are also used in the model aviation and other sectors.

Global Nature of the Supply System

Elements of the supply system for DoD UASs are global in nature, both at the materials and subsystem level. Specific examples of non-U.S. materials and components include such critical items as large focal plane arrays (FPAs) (sourced from Japanese suppliers), composite materials (sourced from Chinese suppliers), and engines (sourced from European and Canadian suppliers).

Cyber Equipment

"Cyber" defines a very broad area that does not fit into the classic construct of the industrial base. Cyber is neither a market nor a market segment, but rather a class of technologies that establishes relationships that we have not seen before—relationships between customers and products, relationships between suppliers, and relationships among different types of products. For this analysis, we define a cyber system as one that can be programmed; that is, operation of the device requires software in addition to computation or communication hardware. Using this definition, the size of the cyber industrial base is very large, containing between 22,000 and 45,000 firms (depending upon the specific screening criteria used).

Issues of Sole Supplier or Constrained Competition

The cyber domain is so large and diverse that it is difficult to develop a generalized conclusion about sole suppliers or constrained competition. Our research leads us to conclude that there are bottlenecks within the sector that may constrain the DoD's ability to obtain the supplies or services required. These bottlenecks include skill shortages, secure semiconductor fabrication, repair and replacement of analog subsystems, and issues concerning intellectual property.

Interdependencies across Programs or Prime Contractors' Supplier Networks

Based on our definition of "cyber," most such systems share common subsystems (e.g., software, microprocessors, interconnect circuits, and memory). U.S. and international standards bodies promulgate design standards at the interface level. However, most inside-the-box designs are based on proprietary standards, which must be licensed for use across manufacturers. The use of these proprietary standards constrains the time-to-market for new designs because real-world business models constrain the adoption or promulgation of the proprietary standard.

Companies with Major Capabilities for Design of Future Products

The industrial base for cyber sector products is large and economically vibrant. The total amount of economic activity in the sector supports our perception that there is no shortage of firms with design capabilities for future products. In addition, the short cycle times for development of new products supports our perception that the industry as a whole will often design around shortages in the supply chain.

Relationship between Military and Commercial Markets

The military and commercial markets for cyber equipment and services exhibit extensive overlap. In many instances, the military procures cyber systems and subsystems from the commercial market. In others, it procures products that incorporate commercial subsystems and components. In yet others, the skills being procured are common, but the products are not. There is, however, a question of the commercial firms' willingness to act as suppliers to the DoD—for reasons ranging from concerns about data rights and audits to the existence of a sufficiently robust commercial market that provides firms with a higher margin.

Global Nature of the Supply System

The cyber industry is global, and the supply chains of firms in the sector are integrated across national boundaries. For example, product specification and design are often done in one country, while manufacturing and testing are done in another. In addition, customer service, which is an increasingly important part of the end-to-end

supply chain and the customer's value proposition, is often located in a third country. Because of the global nature of these supply chains, a large number of non-U.S. citizens work on products with an end use in the United States. Finally, certain sectors, such as manufacturing assembly and packaging, have become specialized industries in themselves, and most of these are based offshore in Asia and Latin America. We have also observed a trend toward using offshore design and software capabilities in Israel and Russia.

Access to Working and Investment Capital at Various Tiers of the Supply Chain

Our tasking also requested that we investigate how key companies obtain access to working and investment capital at the various tiers of the supply chain. Access to working and investment capital varies, depending on specific attributes of a particular firm, such as size, type (public/private), and focus (primarily government contracts, primarily commercial, or mixed). Rather than attempting to examine individual companies in the large universe of companies identified under this task, we chose to look at access to capital in a more general sense. To develop general conclusions, we looked at a sample of companies, including those that act as prime contractors and those that act as subcontractors or suppliers. We examined the financial data of the selected firms, and interviewed company officials at a subset of the firms. From this analysis, we can conclude the following:

- Prime contractors benefit from the availability of contract financing and direct government investment in military products.
- DARPA programs have spurred innovation in design and encouraged the development of military applications. The Intelligence Advanced Research Projects Agency (IARPA) may achieve similar effects on the cyber sector in the future.
- Subcontractors resemble, and in many cases are, commercial firms that fund capital needs through retained earnings and capital markets.
- Within the sectors of the Defense industrial base examined, subcontractors usually fund operations through internal cash flows.
- Prime contractors may pass through contract financing to subcontractors. However, such pass-through arrangements are administratively burdensome on the prime contractors and expose them to financial risk.

Interviews with prime contractors reveal that financing for subcontractors (e.g., milestone financing or payment for investment in tooling) is used only when it is advantageous to the prime contractor (e.g., when a high-demand product is only available

from a small, poorly capitalized supplier or when a critical supplier is in financial distress).

Summary of Conclusions

The conclusions of our analysis of the UAS and Cyber Equipment sectors of the Defense Industrial Base are summarized in the following table.

Summary of Study Conclusions

Category	UAS	Cyber Equipment
Dependence on Sole Suppliers or Presence of Constrained Competition	Few firms capable of designing/building large UASs; many firms capable of building small-to-medium sized UASs. Supplier base capable of producing, but defense industry may not be economically attractive. Obsolescence due to DMS may be more of an issue than sole source.	Little risk of constrained competition today, but industry is subject to rapid obsolescence and dominance of selected few winning technologies in cyber race. Merger and acquisition activity and intellectual property disputes among major commercial vendors also narrowing competition. Short life cycles and shortages in key skills may raise future concerns.
Interdependency Across Programs or Supplier Networks	Growing interdependencies, as DoD attempts to standardize data and communication links and ground control stations.	High levels of interdependency caused by linkage with international commercial business and dependency on specialization in critical human skills.
Major Capabilities for Design of Future Products	Innovation comes primarily from smaller firms and academic research.	Large and economically vibrant industrial base provides a strong capability for design of future products. Industry margins largely dependent on design innovation and forced obsolescence. Tendency for industry to design around supplier issues.
Relationship between Military and Commercial Markets	No broad commercial market yet at the platform level. Extensive relationship at component level, as most UASs rely heavily on commercial components.	Extensive overlap between commercial and military markets, with military markets largely based on “flow-downs” from commercial designs.
Degree to Which the Supply Chain is Global	Many key components provided by international suppliers.	Supply chain is global, often with three or more countries involved in specialized activity (e.g., design vs. manufacturing vs. customer support).
Access to Working and Investment Capital	Prime contractors benefit from government contract financing and direct investment; sub-tier firms resemble commercial firms in that they largely rely on retained earnings and debt for working and investment capital. Flow-through of government contract financing from prime contractors to sub-tier firms is limited to special circumstances.	

Contents

1. Introduction

The Institute for Defense Analyses (IDA) was tasked by the Deputy Assistant Secretary of Defense (Manufacturing and Industrial Base Policy) to perform an exploratory analysis of the supply chains for the Unmanned Aerial Systems (UASs) and Cyber Security Equipment and Services sectors of the Defense Industrial Base as part of its Sector-by-Sector, Tier-by-Tier initiative. Specifically, for these two sectors, IDA was asked to identify:

- Segments of the supply chain that depend on a sole supplier or on constrained competition;
- Interdependencies across programs or across prime contractors' supplier networks;
- Companies that possess major capabilities for design of future products in the sectors;
- The relationship between the military and commercial markets in each sector, including variation across sub-tiers within each sector;
- The degree to which the supply chain is global in nature; and
- How key companies get access to working and investment capital at the various tiers of the supply chain.

To accomplish this task, IDA assembled teams of subject matter experts. These experts used the results of previous studies, interviews with government and industry officials, and their knowledge of the technologies and firms to develop these sector analyses.

Our results are detailed in the following chapters. Chapter 2 presents our analysis of the supply chains for UASs. Chapter 3 presents our analysis for Cyber Security Equipment. Chapter 4 presents an analysis of contract financing, especially as it applies to sub-tier firms. Since each of these sectors is populated by large numbers of firms at both the prime and sub-prime levels, it was not feasible to try to evaluate specific firms in the time available. Instead, we looked at the issue from the larger perspective. Therefore, Chapter 4 provides the analysis of financing for both sectors.

2. Unmanned Aerial Systems

Since the UAS is a relatively new technology, the industry is still in a maturing stage. Clearly defined requirements and an established bureaucracy do not yet exist, and potential uses are still emerging. The U.S. military's interest in UASs has made the United States the world leader in UAS acquisition and use. U.S. firms have over two-thirds of the overall market. Our review identified 125 U.S. producers and developers of UASs, ranging from large Department of Defense (DoD) prime contractors to research laboratories and small firms trying to break into the market. Our review also identified 50 U.S. companies producing UAS payloads, 25 U.S. suppliers of UAS engines, and 25 U.S. UAS avionics manufacturers. Since most of the materials and subsystems are not unique to the UAS sector but are obtained from manned military or general aviation, most issues identified here are not unique to the UAS industry.

The information presented in this exploratory analysis was gathered from interviews with experts in the industry, including representatives from companies that produce or supply parts for UASs, representatives from the Services, and from online and print sources listed in the references.

A. Issues of Sole Supplier or Constrained Competition

Experts interviewed did not identify sole suppliers as an issue at the system or subsystem level. However, supply chain status is an important issue to large UAS developers, as the existence of the position "Director of Supply Chain Strategy" attests. Clearly, supply chains have to be monitored. The Director of Supply Chain Strategy for one major manufacturer noted the importance of knowing the details of the 2nd, 3rd, and 4th tier suppliers. This can be a nearly impossible challenge, with over 8,000 potential suppliers and compounded by the fact that sub-tiers consider their supplier networks proprietary. It is difficult for a major manufacturer to have a complete view of the interdependencies of the supply chain, and to have visibility into all potential nodes that are vulnerable.

Few U.S. companies possess the infrastructure and expertise to produce large UAS platforms. Northrop Grumman (NG), producer of Global Hawk and Fire Scout, is the world's market leader. General Atomics, with the Predator and its derivatives, ranks second. Lockheed Martin's (LM) presence in the market may be understated due to its work on highly classified projects. These large "primes" also dominate the UAS service sector, providing support, hardware and software maintenance and repair, emergency

services, logistics, and ground control. For larger UAS sensor systems, the situation is similar, with only a few companies that serve as prime contractors. For larger UASs, Raytheon has most of the electro-optical/infrared (EO/IR) market, and NG dominates the synthetic aperture radar (SAR) and the signals intelligence (SIGINT) and electronic warfare (EW) markets.[1] The dominance of these large companies as sensor suppliers forces companies such as Boeing, which is making an effort to expand its presence as a UAS producer, to go to their competitors as suppliers.

Energy and innovation in a new industry frequently begins with small start-up companies that form around the intellectual property of one or more innovators. This pattern is seen in the case of small- and micro-sized UASs, for which there is enormous competition, vibrancy, growth, and rapid evolution. This pattern is not true for the large-sized UASs, for which innovation is slower and a few large companies dominate the field. There are only a handful of large UASs, such as Predator and Global Hawk, and they emerged from the Defense Advanced Research Projects Agency (DARPA) nursery, where large and small companies collaborated to build the most innovative design. The vision for large UASs was flexible, adaptable platforms with a capability to quickly change out sensor packages. However, the implementation has become more difficult, and the expected flexibility has been dampened by large integration costs. The reason that the integration of new payload elements has been expensive may be that innovation ended once the risk-averse large DoD contractors inserted themselves into the industry.

As these large prime contractors focus their efforts more on system integration, having a healthy base of small- and medium-sized second-tier suppliers is of growing importance. Opportunities for growth (or survival) in the UAS market will be mostly for subcontractors; however, a recent National Defense Industrial Association (NDIA) survey found that the defense industry can be unattractive to many potential second-tier suppliers given lack of transparency in the bidding and awarding process, underfunded programs, lack of sufficient visibility, and burdensome qualification requirements. Other industries with less burdensome requirements, such as medical, energy, and automotive, are competing for these same qualified firms. These DoD qualification requirements have the potential of creating sole source or constrained competition situations. When competition for critical subsystems is canceled or when only one source is qualified early in the development phase, the system integrator is held hostage to one supplier due to decisions that may have been made years before.

---

[1] The Teal Group's *World Unmanned Aerial Vehicle Systems 2011 Market Profile and Forecast* reports 2011 market shares as follows. For EO/IR: Raytheon, $254 million; FLIR Systems, $44 million; Sierra Nevada, $68 million; for SAR: NG, $189 million; Raytheon, $85 million; General Atomics, $68 million; and for SIGINT & EW: NG, $213 million; BAE, $20 million; Other, $28 million.

We may find examples of constrained domestic competition at the component and materials levels by examining the following question: *If we needed to rapidly ramp up manufacturing capability, where might pinch points exist?* General Atomics states that its current capacity constraints are based on the ability to receive critical subassemblies from their suppliers rather than on production-line capacity. Smaller companies with less procurement clout may be even more constrained in obtaining materials from suppliers. For example, a 2005 worldwide shortage of nylon composites caused problems for AeroVironment in obtaining materials for its small UAS. Specific examples of identified supplier constraints include the following:

- Sony is identified as an important source of large focal plane arrays (FPAs). The recent tsunami adversely affected the supply of these and likely other electronics components in the United States.
- U.S. firms lack the technical capability to produce expanded polypropylene within the tolerances required, forcing Aurora Flight Sciences to buy the material from China for their new small UAS, the Skate.
- Leading manufacturers of precision injection molding machinery are located in Germany, Japan, Austria, and Canada.
- A 2010 General Accountability Office report stated that rare earth metals are ubiquitous materials that are found in many military and civilian technologies, including many electric motors. Rare earth metal supply and processing has, in recent years, been provided almost exclusively by a single non-U.S. source—China. The report projected that rebuilding U.S. capacity to produce/process rare earth materials could take up to 15 years. However, one U.S. company, Molycorp, had reopened mining facilities in the United States, and expected to produce 19,050 tons of rare earth metals by the end of the third quarter of 2010 and, 40,000 tons by 2013. Their March 2012 acquisition of the Toronto-based Neo Materials establishes Molycorp as one of the most technologically advanced, vertically integrated rare earth companies in the world.
- A U.S. Bureau of Industry and Security survey (1997) found that composite manufacturing capability was constrained by a number of sole-source producers and suppliers of defense items. Other manufacturing sources exist, but they had not undergone the DoD qualification process.

In addition to qualification requirements, obsolescence has been cited as being more of an issue than sole source. Because Defense UAS programs rely heavily on commercial components, Diminishing Manufacturing Sources (DMS) can constitute a major supply chain problem as the original components become no longer available in the commercial marketplace. Global Hawk is a major notable example of these DMS issues. Many components of the Global Hawk subsystems are commercial off-the-shelf (COTS), but

the program deferred technology refresh for 13 years. The effect of this deferment was a cost of more than $500 million due to DMS on the components of the system, requiring systems including the ground control station (GCS), communications, and sensor systems to undergo significant redesign, with the consequent burden of a system that is difficult to reintegrate. NG estimates that at least 700 components of the Global Hawk system are affected by DMS.

Figure 1 is a specific example of a Global Hawk system affected by DMS issues in the EO/IR system. The EO/IR Receiver Unit (ERU) consists of a visible EO and an IR sensor, with appropriate optics mounted on a stabilized gimbal. The prime contractor for the EO/IR sensor is Raytheon. The sensor is integrated into the platform by NG. The ERU optics and chassis are a unique Raytheon design. The EO camera and the IR detector assembly are COTS items. The EO camera is manufactured by Basler Vision Technologies, a German company.

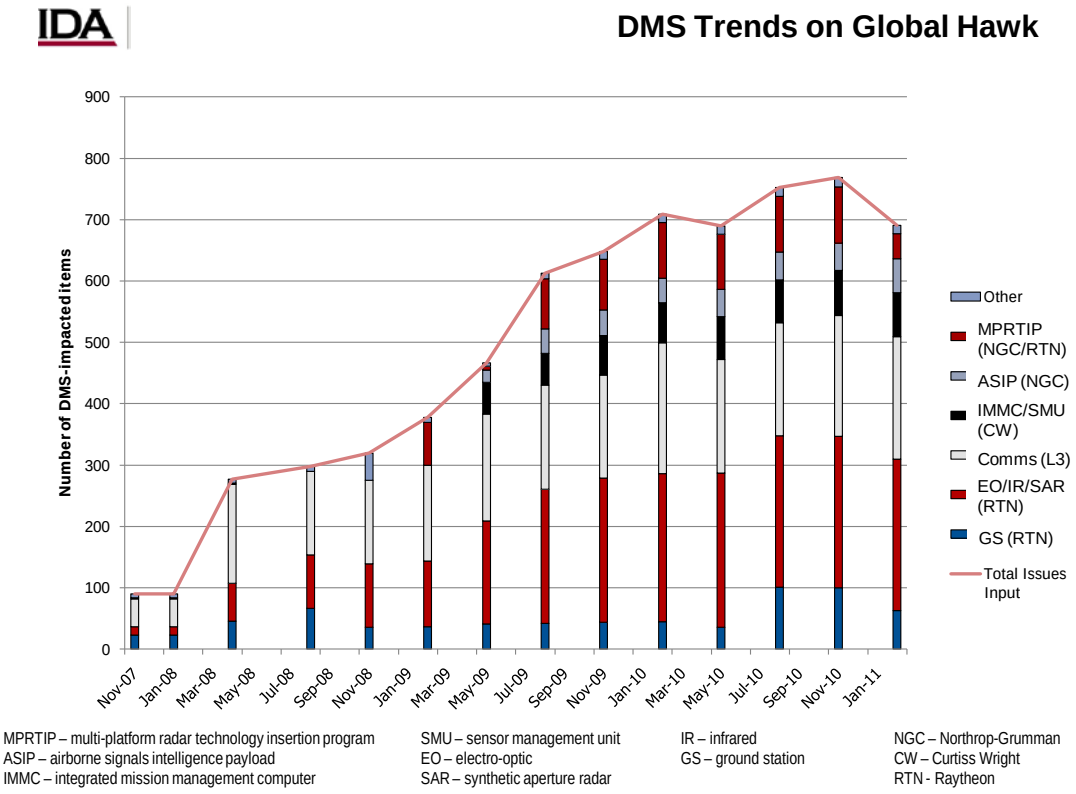

Figure 1. DMS Trends on Global Hawk

In November 2009, Basler sent a memo to its customers and distributors notifying them that the Basler A200 series cameras would be discontinued as of July 30, 2010. The memo stated that "Due to the ongoing demand for improved image quality, reliability, and price, the A200 camera series, including the A201b, the A202k, and all variants, has

reached the end of its product life cycle." The memo goes on to suggest possible replacements and to say that the company would maintain a safety stock level of the affected cameras to be used for warranty and repair purposes and as field replacement cameras. According to NG, this issue is one of the top DMS issues currently affecting the program. In a recent NG briefing on this subject, they claim to have enough units for Low Rate Initial Production (LRIP) Lot 10 but state that a redesign will be needed for LRIP Lots 11 and beyond.

By comparing the detailed technical specifications of the replacement cameras suggested by Basler and given the design constraints present in the Global Hawk ERU, it is clear that they are mechanically and optically incompatible with the Raytheon design and thus not suitable replacements for Global Hawk's LRIP Lot 11 and beyond. At this time, it is not clear how the Program Office and/or the contractors are planning to address this supply chain issue. This example illustrates how the rapidly evolving industrial base driven by commercial requirements rather than DoD needs gives rise to DMS issues.

B. Interdependencies across Programs or Prime Contractors' Supplier Networks

The DoD is currently attempting to standardize elements of UASs. Data links and GCSs are examples of components for which efforts are underway to standardize across multiple programs. Other components are being developed specifically for UASs rather than being leveraged from another sector.

The Tactical Common Data Link (TCDL) is a secure data link needed by the U.S. military to send secure data and streaming video links from airborne platforms to ground stations. It is being developed by two teams—Harris/BAE and L3/Rockwell Collins—for the medium and large platforms. The TCDL can accept data from many different sources and then encrypt, multiplex, encode, transmit, demultiplex, and route these data at high speeds. It uses a Ka narrowband uplink for both payload and vehicle control and a wideband downlink for data transfer. The TCDL was originally designed for the large UASs, specifically the MQ-8 Fire Scout, and for manned non-fighter environments.

Draper Laboratory is working with the Air Force Research Laboratory's Munitions Directorate and the Cryptologic Modernization Programs Office to develop the first secure micro digital data link (SμDDL). The SμDDL waveform is currently being evaluated to become the common data link standard for intelligence, surveillance, and reconnaissance (ISR) sensor platforms that weigh less than 30 lb. Because SμDDL is a non-proprietary, government-owned design, it can be provided as government-furnished equipment (GFE) to the small UAV manufacturers to accelerate protection of these links in small UAS applications. However, providing the SμDDL as GFE may create an issue for new, small UAS developers attempting to break into the market since these firms will have to have a government contract to qualify for this GFE data link. This situation also

creates a huge potential disadvantage to small UAS developers once the civil market in the United States opens up since non-military government use will likely be the largest portion of the civil UAS market.

To some extent, an effort is underway to standardize DoD GCSs. U.S. Navy UAS experts are asking engineers at NG Aerospace Systems in Bethpage, New York, to develop common UAS GCSs to fly the Global Hawk and the Broad Area Maritime Surveillance (BAMS) high-altitude, high-endurance surveillance UASs. BAMS and Global Hawk are based on the NG RQ-4 airframe. The U.S. Army Contracting Command at Redstone Arsenal, Alabama, awarded General Atomics Aeronautical Systems a $9 million contract to integrate a GCS. AAI Corporation in Hunt Valley, Maryland, builds a universal GCS for Army UASs.

Standardization of data links and GCSs can be expected to create interdependencies across programs, with an uncertain effect on the industrial base. Due to security issues, these components are currently made by a very small number of U.S. manufacturers. These security issues constrain competition for these items and force individual programs to tailor their designs to a limited set of prime contractors, hence creating an expensive sole source. For other components, for which the particular manufacturer is not constrained by security concerns, standardization may have an alternative consequence. Aggregate needs for like items across multiple programs may create enough demand to make it economical for second-tier firms to contest the market.

C. Companies with Major Capabilities for Design of Future Products

Our research leads us to conclude that innovation in enabling technologies in the UAS market comes primarily from smaller firms. Even for the larger systems, the innovation and design may have been performed by a smaller company, which was purchased by a larger company once it was determined that the system could be made and would perform as advertised. For example, Ryan Aeronautical, the original developer of Global Hawk, was purchased by NG, and Frontier, the original developer of the A-160, was purchased by Boeing. There are exceptions, however; General Atomics and AeroVironment developed their systems and then maintained the manufacturing themselves.

Larger firms are buying these smaller firms to enter into or expand their share of particular market segments; however, this approach carries the potential risk that innovation may be impeded as the small, independent design teams become part of a larger unit. Recent purchases include

- NG, which purchased the Killer Bee line of UASs from Swift Engineering;
- Boeing, which purchased Insitu, the developer of Scan Eagle;

- Sikorsky, which purchased Schweizer Aircraft;
- L-3 Communications, which purchased Geneva Aerospace, producer of flight control systems, communication systems, and control stations, and Airborne Technologies, producer of the small, foldable Cutlass UAS;
- Textron, which acquired AAI and instantly became the leader in tactical UAS for the Army;
- Rockwell Collins, which purchased Athena Technologies, producer of flight control and navigation systems; and
- Goodrich, which purchased Cloudcap Technology, producer of small inertial measurement sensors and stabilized camera gimbals for manned and unmanned systems.

AeroVironment is an example of a small ($250 million in sales) company that is currently one of the major players in the small UAS market. The company is currently engaged in research on several new platforms, including the high-altitude, long-endurance Global Observer platform (http://www.avinc.com/globalobserver), which is under development for the U.S. Army Special Operations Command, and the DARPA-sponsored Nano Air Vehicle (http://www.avinc.com/nano), a 10-g aircraft that can hover for extended periods.

Academic research is also pushing the technology envelope in nano- and pico-scale UASs. Examples include

- University of California at Berkeley's flying insect (http://robotics.eecs.berkeley.edu/~ronf/MFI/index.html);
- University of Maryland's maple-seed-like platform, (http://diydrones.com/profiles/blogs/university-of-marylands-ulrich); and
- University of Florida's Micro Air Vehicles Laboratory (http://uav.ifas.ufl.edu).

Academic research tends to enable entrepreneur behavior, which promotes entry even as large defense contractors buy up small and successful companies.

D. Relationship between Military and Commercial Markets

At present, the absence of a broad civil or commercial market for UASs is not because of a lack of potential commercial applications but because UASs are not able to routinely access the U.S. airspace system. When airspace procedures for control of UASs are in place, the market can be expected to expand significantly. At the subsystem/ subcontractor level, however, there is a significant relationship between the commercial and defense UAS markets.

Although little or no overlap can be identified between the military and commercial markets on a system or platform level, significant overlap can be identified on the UAS subsystem level. UAS power plants are an example. Most U.S. UAS systems in the larger size classes use engines (or slight variants thereof) found in existing manned commercial, civil, and military systems. One noteworthy requirement for future military internal combustion UAS engines is the use of heavy fuel (for common supply with other military systems). Many off-the-shelf internal combustion engines operate on gasoline.

One might suspect that the added endurance of unmanned systems might lead to changes in engine design. However, this quick study finds that most UAS design changes for improved endurance involve the airframe and airfoil. For example, the A-160 Hummingbird, an unmanned high-endurance helicopter, employs a unique rotor design, with varying stiffness and thickness along its cross section in combination with variable rotations per minute (vs. the variable pitch of a conventional helicopter) to optimize lift for different environments. However, the Hummingbird uses a Pratt & Whitney 207D turboshaft engine that is also found in conventional helicopters, such as the Bell 427.

On the other end of the size scale, man-portable UASs use small displacement internal combustion engines (which we arbitrarily call <150-cc.) or electric motors (brushed, brushless, inboard, outboard). Engines/motors of this size class are also found in the model aviation community. For example, the Desert Aircraft 150-cc. engine (DA-15) is found in Raytheon's Cobra UAS (not a military-designated system). Desert Aircraft is also a prolific supplier of engines to the remote-control modeling community. Small, handheld unmanned systems, like the AeroVironment Raven RQ-11, use electric motors (Aveox 27/26/7 brushless motor). Aveox supplies high-performance electric motors to other sectors, such as civil aviation actuators and medical equipment.

Remote-control model aircraft are often designed for aerobatic performance and short range, whereas military UASs are designed for endurance and reduced signature (visible, acoustic, and radio frequency (RF)). These design differences may lead to notable differences in engine performance and requirements. The internal combustion engines in the modeling community are often loud and are easily heard from distances in excess of 1,000 ft. While this feature may be desirable for the model aviation community, since it is the primary method to warn the operator of loss of engine power, it is an undesirable feature for many military ISR UAS platforms.

Further examples of propulsion systems found in UASs and in other civil or commercial systems include the following:

- The 8,600 lb-thrust Rolls Royce AE3007H turbofan engine is found in the RQ-4 Global Hawk. The AE3007 engine series is found in other civil/commercial aircraft, such as the Cessna Citation X (AE3007C) and Embraer regional jets.

Any unique capabilities attached to the "H" designation found in Global Hawk are unknown.

- The Rolls Royce model 250 Turboshaft engine is used in the NG RQ8-A Fire Scout but is also found in the following: Bell 206, Bell 407, Bell 430, MD500, MD600, Sikorsky 333 & 434, Kiowa Warrior OH-58D, GBA Hawk 4T, Kamov Ka-226, and PZL SW-4.
- The small (<50-lb thrust) turbojet jet engines are found in a few military programs (the Low-Cost Autonomous Attack System (LOCAAS) and the Miniature Air-Launched Decoy (MALD)). However, while these systems are "unmanned," they are munitions and decoys. They are not UASs according to the traditional missions of ISR and hunter/killer. This class of engine is found throughout the model aviation community. Major suppliers are Jetcat (Germany), Technical Directions Inc. (United States), and Jet Central (manufactured in Mexico).
- The 115-HP 4-stroke Rotax 914 class engine (Austria/Germany) found in the Predator (MQ-1B) is also found in many other systems, including very-light and ultralight manned aircraft (Dyn'Aero MCR 4S, France; Europa Aircraft, United Kingdom (UK); and Slipstream Genesis, United States), light helicopters (heli-sport CH-7), and auto-gyros (Magnigyro M-24, Italy).
- The Desert Aircraft DA-150 (150-cc., 16.5-hp) is used in the Raytheon Cobra UAV and in the BAE Kingfisher and Brumby. This class of engine is also commercially available for modelers. Other major suppliers of small (<20-hp) 2- and 4-stroke RC/modeler engines are O.S. Engine (Japan), Thunder Tiger (Taiwan), and Saito (Japan).

E. Global Nature of the Supply Chain

Elements of the supply system for DoD UASs are global in nature at the materials and subsystem levels. However, no sources reported this situation as a significant issue that hindered development of any system. However, it has been an issue for companies with technologies subject to International Traffic in Arms Regulation (ITAR) because it has prevented them from bidding on certain European opportunities.

Specific examples of materials and components integrated into U.S.-made platforms but produced by foreign companies include

- Large FPAs (Sony, Japan),
- Composite materials (China),
- State-of-the-art injection molding machinery (Europe, Japan, and China),

- Rare earth metals (China),
- Engines (UEL, United Kingdom; Thielert, Germany; Rotax, Austria; and Pratt & Whitney, Canada), and
- Payload (IAI for the Plug-In Optronic Payload, Israel; BAE Systems, EADS, and Thales Communications for SIGINT, Europe).

The UAS industry is growing worldwide, and this growth may further accelerate the globalization trend. Companies are making moves to expand their market to both sides of the Atlantic, including

- BAE Systems (UK), which acquired the U.S. company Advanced Ceramics Research. Advanced Ceramics produces small UASs, including Silver Fox and Manta. They are also part of a team developing the TCDL.
- Finmeccanica (Italy), which purchased DRS Technologies, producers of the RQ-15 Neptune and Sentry HP.

3. Cyber Equipment

The cyber threat has been cited as one of the nation's most serious national security challenges.[2] Information and communications technology systems are indispensable to command and control, military operations, and the preservation of critical logistical infrastructure, and we face a host of threats, including cybercrime, espionage, and the denial of service or interruption of mission accomplishment through deliberate cyber attacks by enemy forces. As a result, we now treat cyberspace as an operational domain of warfare.[3]

The information presented in this exploratory analysis was gathered from interviews with industry experts, including representatives from companies who produce or supply designs and software for cyber equipment, software, and services. We also interviewed entrepreneurs and venture capitalists who provide funding for cyber-related technologies and who are intimately familiar with the factors constraining industrial outputs in the cyber sector. Our purpose was to quickly solicit expert opinion on specific questions of interest to the DoD, and, in this effort, we were successful.

"Cyber" is neither a market nor a market segment. It represents a class of technology based on integration among other products and services. The enabling technologies are information, software, communications, and networking.

We must guard against preconceived notions about what cyber is—in particular, a notion that cyber is nothing more than the security of computer networks. Instead, we now perceive cyberspace as a fifth domain of warfare in which we defend the nation and promote our national interests. Because of this study's short duration, we were forced to limit our scope to an operational, *ad hoc* definition of cyber equipment based on the defining characteristic of "programmability"—meaning that the device's function or operation can be fundamentally changed via software, data configuration, or electronic input signals. Thus, for example, a radio would not be considered in scope as a cyber system. Using this definition, approximately 3,000 items of military equipment may be classified as cyber equipment for the purposes of this study.[4]

---

2 Deputy Secretary of Defense William J. Lynn, III, Remarks on Cyber at the RSA Conference (San Francisco, CA, February 15, 2011).

3 General Larry D. Welch, "Cyberspace—the Fifth Operational Domain," *IDA Research Notes* (Alexandria, VA: Institute for Defense Analyses, Summer 2011).

4 David L. Rockwell, *Military Electronics Briefing Book* (Fairfax, VA: Teal Group, July 2011).

A. Issues of Sole Supplier or Constrained Competition

While the short-term risk of sole-supplier vulnerability is slight, we conclude that the cyber security industry is undergoing a rapid metamorphosis because of mergers and acquisitions. We also observe that the cyber equipment industry is unique because of its unusually short life-cycle times, with rapid obsolescence and a dependency upon skilled artisans.

Bottlenecks within the cyber sector may limit the number of suppliers in the supply chain. These potential bottlenecks include

- Skill shortages in cyber security and information assurance, parallel programming and debugging, and network administration networks, including cloud computing environments;
- Secure semiconductor fabrication capabilities;
- Repair and replacement of analog subsystems; and
- Sector-specific factors related to the management and litigation of intellectual property disputes.

Constraints in the cyber industrial base are dominated by a uniquely short life-cycle time—often measured in weeks or even days. In addition, once an artisan can implement a cyber capability successfully, other than packaging, the solution is typically available to the entire world almost instantaneously. Other industrial sectors (e.g., shipbuilding) may take a long time to design and perfect an end item, but, in cyber, the short time cycle distorts factors related to product obsolescence and relative value, which, in turn, adversely affects the capability of the industrial base to respond based on experience and capacity alone. Entrepreneurs reported, for example, that their business has limited room for "second-place" products "trumped" by an adversarial attacker. Every step in the cyber value chain often has a sub-product life cycle driven by obsolescence relative to competing products and the interlocking dependencies of attack and defense in the cyber domain. Entrepreneurs reported, for example, that defensive security products were often developed by attack-oriented analysis of complex vulnerabilities.

Entrepreneurs and venture capitalists provided the following information about the short economic life cycle for cyber products and services:

- Skills are highly perishable, often with time of maximum utility measured in weeks or months.
- The added value of "manufacturing" is declining as a percentage of total life-cycle cost. Assembly and test is now an area for specialization.

- "Build vs. buy" and "replace vs. repair" decisions are influenced by cyclic obsolescence patterns that are usually 12 months or less, making "experience" less valuable.
- Moving from test to production and worldwide distribution can be a matter of "throwing a switch," a process that changes the nature of teamwork.

Software is usually the first element of a cyber system to become obsolete. It is seldom possible to test for absolute correctness or complete invulnerability of the software in a large, complex system. In addition, its production may be the most expensive step in the value chain. From an economic perspective, it is a mistake to confuse "expense" with value, but our purpose is to identify constraints in the industrial base. Dealing with large, complex software systems appears to be a real constraint.

The bottleneck most commonly cited was related to skill shortages. Cyber is strongly manifest in forms of information communications technology, which, in turn, are premised on microelectronics and software advances and on having esoteric "know-what, know-how." Cyber is critically dependent on who brings the "know-what, know-how." Typically, a true artisan must invent an algorithm that is translated into software coding, which runs on programmable hardware. If we were to mistakenly focus on the logistics of producing and distributing the software or the hardware "product" instead of the "know-what, know-how" of the artisan, we would be focusing on an element that is not on the critical path for producing the "next" crucial cyber product. Based on what we were told about obsolescence, the interlocking relationship among attack and defense, short life-cycle times, and the lack of value for second-place products, our thesis is that we can almost ignore the more physical capacity aspects of cyber equipment production and distribution.

Entrepreneurs and venture capitalists stated the following related to skilled worker shortages:

- "Competition for talent" is the single most important factor limiting cyber security product and service development.
- Indicators such as grade point average, academic major, or university name were not viewed as reliable measures of skill.
- Unstructured, apprenticeship-like learning from experience is a common paradigm for training new talent. This approach does not scale well.
- Many workers are non-U.S. citizens.
- Paradoxically, employment opportunity still tends to favor local regions (e.g., California's "Silicon Valley" area).

A second potential bottleneck was related to a perceived need to modernize the nation's secure semiconductor fabrication facilities. This area was explicitly cited by IDA microelectronics experts but not necessarily by entrepreneurs and venture capitalists, a condition we attributed to the lack of focus on the military-specific market by entrepreneurs and venture capitalists.

Components that may be constrained, in priority order, include

- U.S. domestic dynamic random-access memory (DRAM) (but there is no international shortage),
- Semiconductor fabrication processes below 45 nm based on unlicensed intellectual property and trade secrets,
- Semiconductor fabrication machine optics dependent upon non-U.S. technologies and/or assembly,
- Chip-level atomic clocks, and
- U.S. domestic production for high-resolution touch displays.

With the possible exception of U.S. domestic DRAM production, which has been well documented in the trade press, the other constraints listed remain areas for further investigation, particularly in regard to scope and duration of the problem. An important policy issue is also the degree to which U.S. domestic production is affordable or required by the DoD when adequate global, commercial sources appear to be readily available.

Another mitigating factor to consider in relation to the goal of a secure semiconductor fabrication capability is the degree to which modern fabrication technology may obviate the necessity for a controlled-environment, secure fabrication facility (fab). In particular, the use of highly automated fabs based on closed carriers that travel via automated material-handling equipment from tool station to tool station may be the semiconductor equivalent of mini-mills that revolutionized the steel industry two decades ago.

A third potential bottleneck discovered from interviews with entrepreneurs and venture capitalists was related to legacy analog and RF circuits—both in design and repair. In many ways, the physics of analog circuitry, particularly as related to circuit noise abatement, is an art as much as an engineering science, and the past generation of analog circuit design experts is rapidly nearing retirement. The supply of analog circuit experts is not being replenished because of the concentration on digital circuit technologies in today's engineering schools and industrial environments. In addition, the economics of "replace vs. repair" is rapidly reducing the need for technician-level skills—which make these jobs less attractive. While this reduction in need for analog technicians would seem to be a self-mitigating problem, in fact, the demographics of the

skill base was viewed by our interviewees as declining more rapidly than the need. In non-defense work, a typical strategy is to outsource the work, often offshore, because the legacy analog circuitry is viewed as being less critical to corporate success.[5]

The final potential bottleneck is related to the management and litigation of intellectual property disputes and is the most controversial and contentious among the entrepreneurs and venture capitalists interviewed. The issue of cyber patents and its possible deleterious effect on the industry has been well researched[6] and will not be discussed further since no consensus emerged from interviewees about actions to solve the problems. The most common agreement was the stated hope that a natural solution would emerge from the courts, coupled with current congressional action for needed patent reform.

B. Interdependencies across Programs or Prime Contractors' Supplier Networks

To deliver a cyber capability in an operational context, the industrial base must deliver more than the end item. A taxonomy provides a template for data collection beyond the delivered end item and its intrinsic work breakdown structure. In addition to the end item itself, services that depend on "know-what" and "know-how" are delivered. For cyber, identifying the source of the "know-what, know-how" is potentially the most important element, for reasons that were explained previously. All the tangible "stuff" is a manifestation, in some way, of how the "know-what, know-how" was written down or instantiated in the end item.

Once the notion of "know-what, know-how" is accepted as the key resource, constructing the value chain is rather traditional. As an illustration, consider how standards and design documents—which are intellectual property and not tangible manifestations—emerge as a critical dependency across suppliers. Ways and means of getting to an end item are needed. We specify an end item. We typically also specify component elements, which implies an approach (called "architecture") and a design. Thus, the design document itself becomes a critical interdependency in the flow from raw inputs to final output.

Most cyber systems share common subsystems (e.g., software, microprocessors, interconnect circuits, and memory). U.S. and international standards bodies such as the

---

5 As an example, a large domestic semiconductor manufacturer moved all of its analog circuit design work to Israel on or about the year 2000 and then divested completely of this business to a non-U.S. firm approximately five years later.

6 James E. Bessen, Michael J. Meurer, and Jennifer Laurissa Ford, "The Private and Social Costs of Patent Trolls," *Boston University School of Law Working Paper No 11-45* (Boston, MA: September 2011).

Institute of Electrical and Electronics Engineers (IEEE) and the International Organization for Standardization (ISO) promulgate design standards at the interface level. However, most inside-the-box designs are based on proprietary standards, which must be licensed for use across manufacturers. The use of these proprietary standards constrains the time-to-market for new designs because real-world business models constrain the adoption or promulgation of the proprietary standard.

For example, a previously unknown vulnerability in an original equipment manufacturer (OEM)-supplied and managed runtime routine Java virtual machine (JVM) has been discovered and potentially could have been exploited. The original vendor is no longer shipping or supporting the development environment used to program the embedded system. Therefore, there is a significant risk that the user or the original vendor will be unable to locate the appropriate support staff, with the required design expertise in this legacy software, to resolve the vulnerability.

Entrepreneurs and venture capitalists told us of the following interdependencies:

- The market for military-specific cyber equipment is limited, but product demand in the commercial market is comparatively large. As a result, the military market is dependent upon economies of scale and resulting product flowdowns from the commercial market.
- The economics of semiconductor manufacturing favor producers who can maintain the pace of Moore's law in relation to reduction in semiconductor process dimensions. The smaller the chip area, the lower the cost or, potentially, the better the performance. This situation favors large firms over small firms because the large firms (such as Intel, Samsung, and Taiwan Semiconductor Manufacturing Company, Limited (TSMC)) can maintain the level of capital investment required. Even IBM and Texas Instruments have been struggling to keep up with this investment curve, and, as a result, the domestic U.S. production capability has become more concentrated in a smaller number of firms. In the production of application-specific integrated circuits (ASICs), new business models have emerged in which the design firm's business model is "fab-less," in that physical production is outsourced, typically to offshore firms such as TSMC.
- Assembly and test has become a specialized industry, typically offshore in Asia or Central America. For example, Foxconn Technologies, headquartered in Taiwan, has emerged as a dominant player and is currently assembling products for what has been estimated at approximately 1,000 customer firms.
- A strong suspicion among interviewed entrepreneurs and venture capitalists is that intellectual property is being aggressively misappropriated by firms in competitor nations. They voiced special concerns about network routers and

interconnect switches and about computer software. Despite U.S. government sanctions, the entrepreneurs expressed fears about the unfair competition they are seeing in the U.S. domestic market from international low-cost producers.

We investigated the potential for DMS in relation to cyber equipment but did not find any evidence of adverse effect. We attribute this finding to the rapid obsolescence and short life cycle that typifies the cyber sector generally.

C. Companies with Major Capabilities for the Design of Future Products

We considered the design of an ASIC as a specific case study related to the identification of major capabilities for future products. From this case study and from our interviews with venture capitalists, we observed the following:

- The industrial base for cyber sector products is large and economically vibrant. The total amount of economic activity in the sector supports our perception that there is no shortage of firms with design capabilities for future products.
- The short cycle times for the development of new products supports our perception that the industry as a whole will often design around shortages in the supply chain.
- Our interviews yielded a common perception that the DoD should not invest in specific "chosen" technologies for future cyber sector solutions. Our perception is that the unintended consequences from these investments may constrain future innovation. For example, if the DoD were to "choose" a particular approach to cyber defense at the firewall in a network, that choice may discourage more innovative approaches in other areas of the network topology.

In consideration of the large and diverse nature of the cyber sector, IDA also chose to investigate network security appliances as a case study to identify examples of companies that have design capabilities for future products. We were able to identify capabilities for innovation in several distinct tiers, each with its own operating characteristics as follows:

- **Defense Systems Integrators.** Firms including NG, LM, Raytheon, and Rockwell-Collins have design capabilities in cyber that originate with their traditional strength in military electronics.
- **Specialized Military Electronics/Computer OEMs.** Firms including Mercury Computer, Octagon Systems, Ballard Technology, and General Micro have design capabilities that leverage commodity parts in embedded and ruggedized system designs. This tier exploits whatever margins can be obtained by custom engineering and small lot size production from commodity parts. They seldom

have the capital to compete against either multi-nationals or specialized cyber security commercial vendors. In some cases, such as Mercury Computer, the firms have been able to produce products with cutting-edge performance, but this is not generally the case. Instead, they exploit the markets in which military specifications (MILSPECs) and other standards demand specialized solutions or for which they can develop business relationships with major defense integrators. This tier is estimated to have approximately 200 firms with market share significant enough to warrant them as being included in this category.

- **Major Multi-National Commercial Vendors.** Firms including Symantec, Intel (McAfee), Cisco, Juniper, IBM, Hewlett Packard, Microsoft, and Oracle (Sun) have been forced to enter the cyber security marketplace because of the heightened commercial interest in integrated security. This tier has seen a large increase in merger and acquisition activity in the past three years as design capabilities from smaller firms have been integrated through acquisition.
- **Specialized Cyber Security Vendors.** Firms such as Fortinet, Checkpoint, SonicWall, and CrossBeam have strength in point solutions with reasonable market share. Technologies such as ASICs, field programmable gate arrays (FPGAs), system-on-chip architectures, computer-aided design tools, and silicon foundry technologies have lowered the barriers to entry for specialized firms to manufacture products in relatively small lot sizes. IDA projects that firms in this tier may become acquisition targets as larger firms seek to acquire critically short design talent.

D. Relationship between Military and Commercial Markets

As mentioned previously, the military and commercial markets for cyber equipment and services exhibit extensive overlap. In many instances, the military procures cyber systems and subsystems from the commercial market. In others, it procures products that incorporate commercial subsystems and components. In yet others, the skills being procured are common, but the products are not, usually because of MILSPEC or cryptographic requirements.

The size of the cyber industrial base is very large, containing between 22,000 and 45,000 firms, depending upon the specific screening criteria used. Appendix A shows how these results were obtained and reinforces the point that considerable overlap exists between the military and commercial markets for cyber products and services.

According to our discussions with entrepreneurs and venture capitalists, the U.S. government is often considered a customer of last resort for multi-nationals and specialized cyber security vendors. Only the specialized military electronics/computer OEMs specifically market cyber capabilities to the government before other customer

considerations. Reasons cited include concerns about government data rights and audits of proprietary financials and the absence of the type of relationships that exist among commercial firms.

Executives also cited the lack of incentives to pursue government work. They perceive ample commercial opportunities in which their innovation will reward them with higher margins.

E. Global Nature of the Supply Chain

Elements of the supply system for DoD cyber equipment are global in nature at both the materials and subsystem level. However, no sources reported this matter as being a significant issue that hindered the development of any system. However, it has prevented companies with technologies subject to ITAR from bidding certain European opportunities.

During interviews, venture capitalists expressed strong opinions that the global nature of the supply chain, while cost dependent, was essentially irreversible because of the dependency upon the overall microelectronics supply chain. They also stressed the point that a large number of non-U.S. citizens are working on products with an end use in the United States.

The supply chains of many products and services span at least three countries. For example, customer service, an important part of the base, is often not collocated with the product's design and production centers.

Specific examples of materials and components integrated into U.S.-made platforms but produced by foreign companies include the following:

- Microprocessors are designed in Israel, fabricated in the United States, packaged in Vietnam, and tested in Costa Rica.
- Touch panels and other displays are fabricated in Japan.
- Semiconductor fabrication equipment is assembled with German or Japanese optics.

Finally, certain sectors, such as manufacturing assembly and packaging, have become specialized industries in themselves, and most are based offshore in Asia and Latin America. We have also observed a trend toward using offshore design and software capabilities in Israel and Russia.

4. Access to Working and Investment Capital at Various Tiers of the Supply Chain

A. Up-Front Summary and Conclusion

Access to working and investment capital varies depending on the specific attributes of a particular firm, such as size (larger firms often have better access to capital), public or private (public firms have access to capital markets), and the payment process between customers and suppliers. To develop general conclusions, IDA looked at a sample of companies, including those that act as prime contractors and those that act as subcontractors or suppliers. We examined the financial statements of the selected firms and interviewed company officials at a subset of the firms. From this analysis, we can conclude the following:

- Prime contractors benefit from the availability of contract financing and direct government investment in military products.
- Subcontractors resemble, and in many cases are, commercial firms that fund much more of their capital needs through retained earnings and capital markets.
- Within the sectors of the Defense industrial base examined, subcontractors fund operations through a combination of progress payments from prime contractors and internal cash flows.[7]
- Prime contractors may receive progress payments from the government for contract financing provided to subcontractors. However, such pass-through arrangements are administratively burdensome on the prime contractors and expose them to financial risk.

Interviews with prime contractors reveal that financing for subcontractors (e.g., milestone financing or payment for investment in tooling) is used only if there is an advantage to the prime contractor (e.g., when a high-demand product is only available from a small, poorly capitalized supplier or when a critical supplier is in financial distress).

[7] Many of the subcontractors studied reported in their 10K reports that they receive progress payments for products purchased by government customers through prime contracts and subcontracts. It was not possible to quantify how much of their progress payments were from prime contractors.

B. Assessing How Industrial Base Firms Fund Operating Capital

The question of how firms fund working and investment capital is defined more by the specifics of how they get paid by their customers than by what commodity they sell. Although the firm's commodity drives the amount and timing of its financial requirements, the factors that drive funding needs are the length of contracts with customers and the specific services or goods that are bundled together. Consider the UAS for which the ultimate customer is the government, which acquires the system through a series of contracts that span research and development (R&D), production procurement, and potentially sustainment. The government pays the prime contractor through cost-reimbursable and fixed-price contracts that could include a gamut of contract financing payments—from up-front advanced procurement to loan guarantees. Defense contractors selling weapons through Foreign Military Sales (FMS) often receive their revenue up front. Alternatively, if the UAS contractor sold to other private customers, it might not be offered cost-reimbursable contracts for R&D or progress or milestone payments.

At the layer below prime for example, the relationships are business-to-business relationships. Federal Acquisition Regulations (FAR) requirements may flow to many of the subcontractors; however, the transaction is controlled by the private firms. Most commercial industrial firms, including many UAS producers, fund product development, facilities, and working capital internally. In most cases, this funding is done through retained earnings, commercial bank loans, or by offering securities through the capital markets.

As an example, the Ford Motor Company decides to offer a new product some number of years in the future. Its design and market studies are funded through retained earnings or cash raised in the capital markets. This spending steadily increases as the vehicle is designed and the production facilities are built. Even during the first few months of production, the order pipeline (initial customer orders and dealer showroom stock) is financed by Ford even though these vehicles were sold to dealers. Not all commercial firms have the same level of capital requirements as an automobile producer. Retailers such as Amazon are sometimes in the position to use customers to fund part or all of their working capital requirements.

Several practical reasons why private firms fund their own capital needs, in lieu of seeking customer financing, include the following:

- The transaction between businesses is simpler without adding the contractual controls necessary for complex financing.
- Sellers may prefer to have clear retention of any intellectual property associated with the product, and retaining intellectual property may be more contentious if customer financing is involved.

- Financing of suppliers is not necessarily a core business activity of the customer's set of value-creating capabilities and could expose the firm to additional financial risk.

In comparison to the commercial firm's financial requirements, the prime defense contractor may not need to fund much of its product-development cost if it can use R&D contracts to pays these expenses. The government typically purchases production tooling as part of the development contract. As already mentioned, the government funds the contractor's working capital expenses through advanced procurement, progress payments, and performance payments. Consequently, prime contractors have relatively low debt balance sheets when compared to other commercial industrial firms.

If the government is the main customer, a common practice has been to exploit its relative low cost of capital and to fund contractors in exchange for a lower fee. Presently, the Defense Federal Acquisition Regulation Supplement (DFARS) provides guidance for negotiated contract fees. The guidance is for fixed-price contracts, with progress payments to have a fee that is two percentage points lower than those without progress payments. Thus, the financing provided by the government is not without cost for the contractor. For example, contract A offers progress payments and yields 10 percent on revenue and 15 percent on invested contractor capital. Contract B for the same item does not offer progress payments and yields 12 percent on revenue. The contractor will be indifferent between the two contracts as long as the capital required to perform contract B does not exceed the capital required to perform contract A by more than 20 percent.

The FAR allows for, but does not require, prime contractors to request progress payments for subcontractors. In such a case, the prime appears to be a pass-through for the payment, and the government has as direct partial title to the subcontractor's work in process. The prime can receive the progress payment on the sub's behalf but must pay the sub within 30 days of the request. Note that the prime cannot receive progress payments based on the subcontractor's incurred costs—only on the amount to be paid. Thus, if the government is charging the prime two percentage points of contract cost for financing, it is expected that the prime will negotiate similar or better pricing with the sub.

C. Empirical Methodology

We expect prime defense contractors to have relatively low operating funding requirements and a higher level of cash available for investment or shareholder payout compared to commercial firms. The strategy for constructing metrics to test this hypothesis starts by considering the firms' uses and sources of cash. The firms in this analysis mostly need cash for investing in new products, working capital, shareholder payout, and acquisitions. Mergers and acquisitions are excluded in this analysis.

Differences are observed by looking at the financial statements of publicly traded firms in the various tiers of the Defense industrial base.[8]

Product engineering appears in the income statement if it is material to the firm's financial performance. We expect prime contractors to have relatively high levels of customer-sponsored R&D expenses. Generally, R&D expense is associated with activities that will affect the revenue in future periods.[9] Firms in the sample generally associated expenses that were aimed at generating future revenue with R&D. For the most part, these expenses were not customer-sponsored. Customer-sponsored R&D was recorded in cost of goods sold, since the revenue for the expense was also recorded in the same period. Thus, the R&D expense is a good—though not perfect—partial indicator of the firm's capital requirement.

Capital expense will similarly be lower for prime contractors than purely commercial industrial firms. The key difference is unique tooling, the construction of which the government funds directly.

Working capital is defined as short-term assets less short-term liabilities, but, in terms of the important operating accounts, it is accounts receivable plus work in process and finished goods inventory less accounts payable. Accounts receivable represent that portion of the firm's revenue that has not been paid. Accounts payable are invoices received that the firm has not yet paid.

Most defense prime contractors invoice on a work-as-completed basis and receive a progress or performance-based payment of 80–95 percent of the cost incurred.[10] The remainder of the amount owed is paid when the item is delivered and accepted by the government.

Firms are expected to put cash to work or return it to their shareholders as either share repurchases or dividends. The choice is dependent upon which action will deliver the highest returns to the firms' owners. Firms can also use cash to reduce debt.

Financial reports can be used to analyze capital financing requirements trends through the tiers of the industrial base. To do this analysis, we use the financial statement database in CapitalIQ and compare financial metrics for the different tiers. The metrics, intended to detect the financing characteristics of the different tiers of the industrial base,

---

8 Although privately held firms were excluded from this analysis due to the lack of available information, these findings will apply to such firms. However, a privately held firm's access to capital will depend on its ability to borrow directly from a bank or receive equity from private investment.

9 Generally accepted accounting practice requires R&D costs to be expensed in the period in which these costs are incurred, in contrast to capital expenses, which are amortized over a schedule specific to the asset type.

10 Contractors may also start booking revenue on a milestone completion basis.

are derived from the financial statements of the representative firms in the different tiers. The financial performances of similar firms are aggregated into representative indices to facilitate comparison and to smooth out the variations across individual firms. The methodology description is expanded below.

Expense and cash metrics are normalized on a percentage-of-revenue basis. Cash-use metrics are also normalized as a percentage of operating cash flow. The reason for the two bases will become clear later in the analysis. Normalizing metrics allows the tier indices to be directly compared. Using indices circumvents the idiosyncrasies of comparing individual firms, where one firm's metrics may reflect that it is much more efficient than its competitors. The indices should smooth out the differences in operating efficiencies between firms and simply capture the rough differences in operating characteristics between industry tiers.

The four indices were constructed from the firms listed in Table 1. The prime contractor index includes firms that are predominantly paid by the government through contracts. Thus, Boeing is excluded because its commercial aircraft unit is so large that it alters the metrics dramatically. The subcontractor index consists of firms that have a mix of prime contracts and subcontracts with the government and commercial sales to non-military industrial customers. The group is broken up into two subgroups: subsystems and components. The subsystems tier is composed of companies that have a mix of prime contracts and subcontracts for integrated subsystem equipment such as sensors and avionics. It also includes electronics manufacturing services firms. The components tier is composed of firms that mostly have subcontracts to manufacture or fabricate components used by the prime contractor to build the system. For example, Precision Castparts forges landing gear that Heroux-Devtek might machine into a finished part. It is not clear that the forgers are a third tier in the chain since, in some cases, they have long-term agreements with the prime contractor. In some cases, the prime contractors even have long-term agreements with the firms that supply specialty metals to the forgers.

D. Empirical Analysis of Public Firms in the Defense Industrial Base

Table 2 lists the first set of operating capital use metrics for the three indices. The capital-use metrics indirectly show how firms finance their working capital. Firms that have similar capital intensity and fund most of their capital needs internally will have higher product development expenses and working capital than firms that use customer financing to fund operations. The comparison shows that the primes spend less, as a percentage of revenue, on new products in the form of R&D and capital equipment than the two subcontractor indices. This result is consistent with the finding that prime contractors rely on government contracts to directly fund new product development while subcontractors spend more of their own capital on these requirements.

Table 1. Sample Firms Used To Construct Tier Indices

	Subcontractors (Tier 2 and Lower)		
Prime Contractors	**Subsystems**		**Components**
General Dynamics (GD)	API Technologies	ITT	Alliant Techsystems
LM	Astronics	KEYW Holding Corp.	Ceradyne Inc.
NG	Cubic Corporation	Kontron	GKN
Raytheon	Curtiss-Wright	L-3 Communications	Heroux-Devtek
	Ducommun	Mercury	Hexcel
	Edac Technologies	Moog	Ladish
	ELBIT	RadiSys	LMI Aerospace
	Esterline Technologies	Rockwell Collins	Precision Castparts
	FLIR	Sparton Corp.	Spirit AeroSystems
	Goodrich	Sypris Solutions	
	Harris	Teledyne Technologies	
	Honeywell Int'l	Triumph Group, Inc.	

Table 2. Operating Capital Use Metrics

		Subcontractors	
Annual Expense % Revenue	**Prime Contractors**	**Electronics**	**Components**
R&D	2.5%	8.0%	2.6%
Capital Expense	1.9%	2.5%	4.3%
Working Capital (WC)[a]	14.2%	27.5%	30.2%
Customer Advances/Revenue	11.5%	4.3%	3.6%

[a] *WC = Accounts Receivable + Inventory – Accounts Payable*

Most of the firms in both subcontractor indices spend a mix of customer and internal funds on R&D. For example, 58 percent of Rockwell Collins R&D expense is customer funded, 80 percent of which is for government material. However, the firms do not indicate how much of the government content is funded by prime contractors. The R&D expense metric was adjusted to reflect, as best possible, company-funded R&D. The difference in R&D expense between the "Electronics" and "Components" firms is reflected in the "Electronics" group's level of integration of the products. The Electronics firms sell content that contains more intellectual property than the Components group, which produces many parts that are designed by the prime contractors.

Prime contractors also have a lot less capital tied up in working capital—again consistent with the prime contractors' use of the government contract financing to fund working capital. By examining the individual annual reports for the firms in the

subcontractor indices, it is clear that they receive some level of progress payments on subcontracts. However, they do not differentiate between the progress payments on prime contracts and subcontracts. Ladish does not have prime contracts for its forgings but indicated that it required progress or milestone payments.

Note also that "Customer Advances/Revenue" is much higher for prime contractors than for the two subcontractor indices. "Customer Advances" is a liability account that is often used to reflect revenue and cost-of-sales timing mismatches. This metric is an indirect measure for the level of progress and performance payments relative to the contractor's total business.

Table 3 shows the operating capital source metrics. Again, these metrics show indirectly how firms fund operating capital. As in the previous capital use metrics, firms that must fund all of their product development expense and working capital will need to borrow more than firms that receive customer financing. This statement assumes most firms have similar views on using debt financing in lieu of or in addition to equity financing.

Table 3. Operating Capital Source Metrics

Metric	Prime Contractors	Subcontractors	
		Electronics	Components
Debt/Assets	13.9%	15.0%	18.3%
Debt/Capital	34.0%	23.8%	27.0%

The metrics show that the prime contractors borrow less, as a percentage of assets, than the subcontractors, although the difference is not great if measured relative to total assets. The differences presumably reflect, in part, the higher level of customer financing for prime contractors relative to Electronics and for Electronics relative to Components. There are other reasons for setting a firm's capital structure at a specific level. For example, firms that expect to acquire another firm in the future may carry less debt and thereby have more debt capacity so that it can be raised when needed without adversely affecting the firm's credit quality. In contrast, since 2008, many commercial firms have exploited the low debt costs to raise cash cushions. By using indices composed of several firms, the idiosyncrasy of individual firm strategy has been eliminated.

Debt level measured as a percentage of capital is higher for prime contractors than for subcontractors. This can be explained by examining Table 4, which revisits the use of cash with metrics that are normalized to operating cash flow. The first metric is the ratio of product investment expenses to operating cash flow. Again, this metric is consistent with the metrics in Table 2; prime contractors invest about half as much of their cash flow in new products as the two categories of subcontractors do, which is also reflected in

the "Cash to Shareholders" metric. Prime contractors generate a great deal of cash flow, and yet they do not need to put it into new products since the development of these products is directly funded by their customers. This partially explains why prime contractors are returning 3 to 60 times the cash to shareholders as subcontractors do. Thus the difference in shareholder payouts partially explains the high debt-to-capital ratio in Table 3.

Table 4. Cash Use as a Percentage of Operating Cash Flow

% Adjusted Operating Cash Flow[a, b]	Prime Contractors	Subcontractors	
		Electronics	Components
Investing in the Business: R&D, Capital	44.5%	76.2%	84.6%
Cash to Shareholders: Dividends & Share Repurchase, Net of Debt Level Changes	-62.1%	-22.2%	-0.9%

[a] Operating cash flow is adjusted to exclude R&D expense—i.e., R&D is capitalized.

[b] The % values can sum to greater than 100 percent—this implies that debt is issued.

There are other reasons why the two tiers differ in any given year. For example, the recent recession gave firms without customer financing a reason to conserve cash and suspend or lower share repurchases and dividends. Extending the metric to average over the 10 years ending in 2010, the prime contractor's payout rate is about 25 percent while the subcontractor's payout rate is about 0 percent. At the peak of the defense spending cycle, prime contractors were paying out significantly more than subcontractors. The peak of the defense cycle corresponded with the recession and financial crisis of 2008. In contrast to the prime contractors, these events put pressure on commercial firms to conserve cash.

There are other less measureable matters to consider in assessing the relative access to capital for the lower industrial base tiers. Many of the lower tiers have financial covenants associated with their debt. For example, most of the Components firms had covenants requiring the maximum leverage, the minimum market capital value of the firm, or interest coverage. While all of the firms examined were in compliance with their covenants, the smaller firms indicated that these restrictions posed a risk to the firm. For example, one acquisitive firm indicated that if it were forced to write down its substantial goodwill, this requirement could potentially cause it to breach the net-worth covenant. The larger subcontractors and prime contractors did not indicate that their covenants posed risks to the firm.

E. Interviews with Selected Firms

Interviews with several defense contractors and subcontractors were conducted to corroborate and verify the financial analysis performed in the previous section. From the

prime contractor set, Boeing, LM, Huntington Ingalls, and General Dynamics (GD) were contacted. All but GD responded to the request for an interview. Of the firms in the subcontractors' index, only Mercury agreed to an interview.

LM Aeronautics, Boeing, and Huntington Ingalls reported that they provide milestone payments to sole-source suppliers. All three firms said that milestone payment plans are based on a business case where the prime contractor seeks a cost benefit from the supplier for the financing. For example, suppliers that provide long-lead components, such as complex titanium forging, can benefit from customer financing provided by the prime contractor. This finding is consistent with Ladish's statement in its annual report that it requires milestone payments for long-lead components.

The primes that were contacted considered financing suppliers as part of the negotiated transaction price of the component. The prime contractors expect a lower unit price from suppliers to which they provide financing, such as milestone or progress payments, than from suppliers who are paid upon delivery invoice. The FAR requires that the financing terms offered to the subcontractor be at least as favorable as those offered by the government to the prime. This requirement appears to ensure that interdivisional work authorizations (e.g., between NG Aircraft and the Electronics Division) do not pad transfer prices with extra profit. However, the provision also promotes the tradeoff between fee and financing in the price that the government implicitly charges for contract financing. The primes should negotiate lower prices from the subcontractors they finance to compensate for their cost of capital.[11]

Primes reported that they provided financing for three reasons:

- Higher short-term profits,
- Higher long-term profits, and
- Ensuring short-term supply from distressed critical suppliers.

Financing the suppliers contributes to higher short-term profits by lowering the total cost of the transaction. Typically, these profits are achieved because the buyer's cost of capital is lower than that of the supplier. Prime contractors have lower cost of capital than many of their suppliers because their relationship with the government provides them with strong and relatively stable cash flows. Table 5 lists the most recent Standard and Poor credit ratings for those firms in Table 1 that have ratings. The lowest rating for a prime contractor is BBB+ while about half the subcontractors have ratings that put them below investment grade.[12]

---

[11] DFARS reference.

[12] Investment grade is any rating at or above BBB–.

Table 5. S&P Credit Ratings on Selected Firms

Primes	Rating	Subs	Rating
GD	A	Alliant Techsystems	BB
LM	A-	API Technologies	B+
NG	BBB+	Ducommun	B+
Raytheon	A-	Esterline Technologies	BB+
		FLIR	BBB-
		Goodrich	BBB+
		Harris	BBB+
		Hexcel	BB+
		ITT	BBB+
		L-3 Communications	BBB-
		Moog	BB
		Precision Castparts	A-
		Rockwell Collins	A

There are cases where the prime contractor finds a valuable technology or service from a small, undercapitalized supplier. While the prime contractor may not be in a position to obtain beneficial pricing from the small supplier, it may be able to forge a long-term strategic relationship by providing working capital investments. The benefits are likely to be uncertain and long term. This type of supplier financing is relatively rare.

Finally, a common reason to finance a supplier is to maintain the supply of critical components. A supplier in financial distress, possibly near or in Chapter 11 bankruptcy protection, will still be able to deliver parts but may need the customer to pay up front. This type of financing is a common business practice and is not unique to aerospace and defense. It is also not the type of financing the contractor should be willing to do long term since the distressed supplier is not only a financial risk but also an operation risk in meeting the production schedule. Prime contractors are likely to seek alternatives to a distressed supplier.

Mercury Computer confirmed that most of their transactions with prime contractors are invoiced on delivery, as is done with their commercial customers. Milestone payments are common, however, for development projects with primes.

The evidence shows that contractors and their suppliers are behaving opportunistically, as one would expect of commercial firms. To an extent that we could not quantify, prime contractors provide some contract financing to subcontractors. From the interviews, it does not appear to be the prime contractor's preference to provide supplier financing, due to the risk in operating as a financial services company to suppliers and the additional administrative expense involved. The financial risk emerges because one side of the contract pair could be cancelled due to subcontractor default or if

the government cancelled for convenience, leaving claims in place that would have to be resolved. For the prime contractor, having to maintain records to ensure that the proper payments are made and recovered and to provide sufficient supporting documentation creates added work that may unnecessarily divert management focus from the main value the prime contractor provides to the customer.

Furthermore, based on the relative profitability of the primes and the subs, it does not appear that one tier is exploiting the other. Table 6 shows the operating margin and the free cash flow return on capital for the three indices. The primes have the lowest margin but relatively high cash flow return. The Electronics subcontractors have higher margins and slightly higher cash flow return, while the Components subcontractors have higher margins but lower cash flow returns. There are many business drivers that affect the firms' profits; however, the prime contractors appear to be making a lower margin in return for using the government's capital to fund operations.

Table 6. Defense Sector Operating Margin and Free Cash Flow Return on Capital

		Subcontractors	
	Prime Contractors	Electronics	Components
Operating Margin (% of Revenue)	9.7%	11.5%	84.6%
Free Cash Flow Return on Capital	13.8%	14.4%	11.9%

F. Section Summary and Conclusion

Prime contractors generally have access to low-cost working and investment capital from the government. The evidence for this finding is reflected in the relatively light level of product development spending and working capital on prime contractors' financial statements. These costs are directly reduced relative to commercial industrial firms through contract financing (e.g., progress payments) and R&D contracts (which lower internal R&D and capital expenses). The FAR allows primes to receive progress payments for contract financing provided to subcontractors; however, it is not clear to what extent prime contractors provide this type of financing. Further removed from the prime level, access to capital is determined by the credit and equity markets.

Most of the business transactions below the prime contractor level are best thought of as commercial, implying that financing is based on the profit opportunity afforded through extending credit. The prime contractor can receive government progress payments if it provides financing to subcontractors—but at a cost of two percentage points of fee based on cost. Thus, the prime contractor should insist on similar or better pricing for financing the subcontractor (i.e., the prime contractor should receive a spread for providing this service).

Access to working and investment capital varies depending on the specific attributes of a particular firm, such as size (larger firms often have better access to capital), public or private (public firms have access to capital markets), and the payment process between customers and suppliers. To develop general conclusions, IDA looked at a sample of companies, including those that act as prime contractors and those that act as subcontractors or suppliers. We examined the financial statements of the selected firms and interviewed company officials at a subset of those firms.

The commercial relationships between prime contractors and subcontractors or supplier to supplier are driven, to a large extent, by transaction costs. If a buyer were to receive a net benefit by offering early payments or some other type of contract financing to the supplier, this arrangement will be part of the transaction. However, the financial risk and cost to administer a high volume of these types of financing payments is not negligible. For large buyers with many supplier transactions, offering working capital financing starts to turn the firm into a financing company. While several large industrial firms have financing divisions that lend to retail customers, it is not common for customers to finance suppliers.

From this analysis, we can conclude the following:

- Prime contractors benefit from the availability of contract financing and direct government investment in military products.
- Subcontractors resemble, and in many cases are, commercial firms that fund much more of their capital needs through retained earnings and capital markets.
- Within the sectors of the Defense industrial base examined, subcontractors fund operations through a combination of progress payments from prime contractors and internal cash flows.[13]
- Prime contractors may receive progress payments from the government for contract financing provided to subcontractors. However, such pass-through arrangements are administratively burdensome on the prime contractors and expose the prime contractors to financial risk.

Interviews with prime contractors revealed that financing for subcontractors (in a form such as milestone financing or payment for investment in tooling) is used only if there is an advantage to the prime contractor (e.g., when a high-demand product is only available from a small, poorly capitalized supplier or when a critical supplier is in financial distress).

---

[13] Many of the subcontractors studied reported in their 10K reports that they receive progress payments for products purchased by government customers through prime contracts and subcontracts. It was not possible to quantify how much of their progress payments were from prime contractors.

Appendix A.
A Methodology for Characterizing the Department of Defense (DoD) Cyber Industrial Base

This appendix describes the collection and analysis of existing data that could be used to gain insight into an inductive process to define the DoD cyber or information communication technology (ICT) industrial base. The methodology begins with the existing data structures used to characterize the U.S. industrial base. The methodology then looks at the nominal "fit" of other descriptors of DoD purchases of goods and services that are presumed to incorporate programmable devices or are part of the supply chain by which such devices are created, assembled, manufactured, tested, packaged, used, or sustained as part of DoD systems. Finally, we discuss how the current data structures describing ICT/cyber "things" or "services" can be used to identify specific entities that supply such "things" or "services" that are representative of capabilities upon which DoD relies for present and future systems.

Industry Census Data

Several schema currently in use describe the entities that make up the U.S. industrial base. The most commonly used schema are as follows:

- **The North American Industry Classification System (NAICS)**. The NAICS was developed under the auspices of the Office of Management and Budget (OMB) and maintained by the U.S. Census Bureau.
- **The Standard Industrial Classification (SIC) System**. The SIC was replaced in 1997 by the NAICS, but is still used in many U.S. government agencies (see for example, the Occupational Health and Safety Administration's website, which maintains the SIC codes and uses them for the administration of occupational health and safety regulations (http://www.osha.gov/pls/imis/sic_manual.html).

The NAICS schema contains multiple categories of commercial activity that span the range of activities that might be included as part of the ICT/Cyber industrial base. Table A-1 lists these categories. This table does not include categories that would incorporate large numbers of programmable devices, such as aircraft, command and control systems, or sensors for weapon systems.

Table A-1. Selected NAICS Codes and Descriptions for "ICT/Cyber Technology Entities"

NAICS Code	Industry Description
238210	Electrical Contractors and Other Wiring Installation Contractors
333295	Semiconductor Manufacturing
334111	Electronic Computer Manufacturing
334112	Computer Storage Device Manufacturing
334113	Computer Terminal Manufacturing
334119	Other Computer Peripheral Equipment Manufacturing
334418	Printed Circuit Assembly (Electronic Assembly) Manufacturing
334515	Instrument Manufacturing for Measuring and Testing
334611	Software Reproducing
423430	Computer &Computer Peripheral Equipment & Software Wholesalers
423690	Other Electronic Parts & Equipment Merchant Wholesalers
454113	Mail-Order Houses
517110	Wired Telecommunications Carriers
517911	Telecommunications Resellers
517919	All Other Telecommunications
518210	Data Processing, Hosting, and Related Services
541511	Custom Computer Programming Services
541512	Computer Systems Design Services
541513	Computer Facilities Management Services
541519	Other Computer Related Services
541618	Other Management Consulting Services
611420	Computer Training
611519	Other Technical and Trade Schools
811212	Computer and Office Machine Repair and Maintenance

The SIC system also includes a number of categories, listed in Table A-2, that describe commercial activity that might be included in the ICT/Cyber industrial base.

Table A-2. Standard Industrial Classification Codes for ICT/Cyber Technology Entities

Industry Group 357: Computer and Office Equipment	
3571	Electronic Computers
3572	Computer Storage Devices
3575	Computer Terminals
3577	Computer Peripheral Equipment, Not Elsewhere Classified
3578	Calculating and Accounting Machines, Except Electronic Computers
3579	Office Machines, Not Elsewhere Classified
Industry Group 737: Computer Programming, Data Processing, and Other Computer-Related Services	
7371	Computer Programming Services
7372	Prepackaged Software
7373	Computer Integrated Systems Design
7374	Computer Processing and Data Preparation and Processing Services
7375	Information Retrieval Services
7376	Computer Facilities Management Services
7377	Computer Rental and Leasing
7378	Computer Maintenance and Repair
7379	Computer Related Services, Not Elsewhere Classified
Industry Group 381: Search, Detection, Navigation, Guidance, Aeronautical, and Nautical Systems, Instruments, and Equipment	
3812	Search, Detection, Navigation, Guidance, Aeronautical, and Nautical Systems and Instruments
Industry Group 382: Laboratory Apparatus and Analytical, Optical, Measuring, and Controlling Instruments	
3821	Laboratory Apparatus and Furniture
3822	Automatic Controls for Regulating Residential and Commercial Environments and Appliances
3823	Industrial Instruments for Measurement, Display, and Control of Process Variables; and Related Products
3824	Totalizing Fluid Meters and Counting Devices
3825	Instruments for Measuring and Testing of Electricity and Electrical Signals
3826	Laboratory Analytical Instruments
3827	Optical Instruments and Lenses
3829	Measuring and Controlling Devices, Not Elsewhere Classified
Industry Group 386: Photographic Equipment And Supplies	
3861	Photographic Equipment and Supplies
Industry Group 387: Watches, Clocks, Clockwork Operated Devices, and Parts	
3873	Watches, Clocks, Clockwork Operated Devices, and Parts

Some overlap occurs in the two schemas, but important differences and distinctions between the two are also apparent.

Government Procurement Activity Codes

The U.S. government also applies a data schema to monitor its acquisition and procurement activities. The Product and Service Codes (PSC) Manual issued by the General Service Administration's (GSA) Office of Governmentwide Policy for use with the Federal Procurement Data System (FPDS) contains a schema that is applied to all U.S. government procurements of products and services. Table A-3 lists those PSCs and the class level covering DoD procurements of products and services rich in programmable devices or associated with the infrastructure to produce those products and services. The specific line items within each class of interest cumulate to more than 1,300 individual products or services.

Table A-3. ICT and Cyber Technologies Product and Service Codes

Product and Service Codes (PSCs)	
A	Research and Development
B	Special Studies and Analyses
D	Automatic Data Processing and Telecommunication
E	Purchase of Structures and Facilities
H	Quality Control, Testing, and Inspection
J	Maintenance, Repair, and Rebuilding of Equipment
K	Modification of Equipment
T	Photographic, Mapping, Printing, and Publications
U	Education and Training
Federal Supply Codes (FSCs)	
10	Weapons
11	Nuclear Ordnance
12	Fire Control Equipment
13	Ammunitions and Explosives
14	Guided Missiles
15	Aircraft and Airframe Structural Components
16	Aircraft Components and Accessories
17	Aircraft Launching/Landing/Ground Handling Equipment
18	Space Vehicles
19	Ships, Small Craft, Pontoons, and Floating Docks
20	Ship and Marine Equipment
23	Ground Vehicles, Motor Vehicles, Trailers, Cycles
25	Vehicular Equipment Components

Federal Supply Codes (FSCs)	
26	Tires and Tubes
28	Engines, Turbines, and Components
29	Engine Accessories
30	Mechanical Power Transmission Equipment
32	Woodworking Machinery and Equipment
34	Metalworking Machinery
35	Service and Trade Equipment
36	Special Industry Machinery
38	Construction, Mining, Excavating, Highway Maintenance
39	Materials Handling Equipment
41	Refrigeration, Air Conditioning Equip.
42	Fire Fighting, Rescue, and Safety Equipment
43	Pumps and Compressors
44	Furnace/Steam Plant/Drying Equipment, Nuclear Reactors
45	Plumbing, Heating, and Sanitation Equipment
49	Maintenance and Repair Shop Equipment
52	Measuring Tools
58	Communications, Detection and Coherent Radiation
59	Electrical and Electronic Equipment Components
60	Fiber Optics Materials and Components
61	Electric Wire, and Power and Distribution Equipment
62	Lighting Fixtures and Lamps
63	Alarm, Signal, and Detection Systems
65	Medical, Dental, and Veterinary Equipment
66	Instruments and Laboratory Equipment
67	Photographic Equipment
69	Training Aids and Devices
70	ADP Equipment Software, Supplies, Equipment
74	Office Machines
75	Office Supplies and Devices
76	Books, Maps, and Other Publications
81	Containers, Packaging, and Packing Supplies

Federal Procurement Data System Extracts

The GSA maintains the FPDS for tracking overall U.S. government compliance with broad policy goals and objectives regarding the procurement of goods and services.

These goals include use of competitive processes, use of procurement preference programs, use of American firms, and use of special legal authorities. The goal is to provide the OMB, the Office of Federal Procurement Policy (OFPP), Cabinet Secretaries and Agency Heads, and members of Congress with trailing indicators of overall compliance with statutory and declaratory acquisition and procurement goals and objectives.

The FPDS also records information for each contract, grant, or "other transaction" that allows inference about the product or service actually being acquired. The FPDS records the FPDS Product or Service Code and Product or Service Description, the NAICS Code and NAICS Description, and the identity of the performing activity. These data permit the identification of active defense industrial base participants, including both government agencies that provide products and services to other DoD entities and commercial or academic/non-profit organizations that deliver products and services to DoD.

For FY 2010, a search of the FPDS for DoD procurements resulted in the identification of 3,625,551 transactions totaling more than $367,139,526,814.61. In principle, it should be possible to query the FPDS to extract the PSC and NAICS codes to identify the number of transactions, dollar values, and individual organizations that constitute the ICT/cyber industrial base under active contract to DoD. However, the FPDS limits reports to fewer than 15,000 lines, and it was not possible to generate a DoD-wide search for a single day that did not exceed the threshold. Individual DoD contracting agencies will have to be extracted on a day-by-day basis to build a good profile of the ICT/cyber industrial base under direct contract to DoD. By focusing on contract actions to companies with specific PSCs and/or NAICS codes, we will be able to describe the relatively recent members of the direct DoD industrial base.

Central Contractor Registration Database

The GSA also maintains the Central Contractor Registration (CCR) database of U.S. government contractors, prospective contractors, and grantees. Established pursuant to the FAR part 4.11, this database includes many entities that may not be active U.S. government or DoD contractors but may have been contractors in the past or may be current subcontractors who have registered because of contractual requirements imposed by a prime contractor or in anticipation of becoming a DoD contractor in the future. The CCR, therefore, represents a more complete collection of entities that constitute the gross defense industrial base.

The CCR publishes a complete listing of all registrations on a quarterly basis to facilitate compliance with the Freedom of Information Act (FOIA). The FOIA file provides identification information on current and potential federal government contractors and grantees and on other current or potential suppliers of products and

services to the federal government (e.g., federal agencies, state and local governments, international organizations, and commercial activities). Among the descriptive data included on each entity are NAICS, SIC, and PSC Codes. The current CCR contains 620,236 registrants.

Table A-4 shows the results of a search of the CCR FOIA file, which identified the indicated number of entries (see Column 3) for each of the NAICS codes of interest.

Table A-4. NAICS Codes and Definitions of Interest as "Cyber Technology Firms"

NAICS Codes	NAICS Description	# of Entries
238210	Electrical Contractors and Other Wiring Installation Contractors	22571
333295	Semiconductor Manufacturing	459
334111	Electronic Computer Manufacturing	3020
334112	Computer Storage Device Manufacturing	1647
334113	Computer Terminal Manufacturing	851
334119	Other Computer Peripheral Equipment Manufacturing	3226
334418	Printed Circuit Assembly (Electronic Assembly) Manufacturing	1896
334515	Instrument Manufacturing for Measuring and Testing	2596
334611	Software Reproducing	1128
423430	Computer &Computer Peripheral Equipment & Software Wholesalers	7258
423690	Other Electronic Parts & Equipment Merchant Wholesalers	5299
454113	Mail-Order Houses	735
517110	Wired Telecommunications Carriers	4637
517911	Telecommunications Resellers	3232
517919	All Other Telecommunications	3917
518210	Data Processing, Hosting, and Related Services	10229
541511	Custom Computer Programming Services	27007
541512	Computer Systems Design Services	27331
541513	Computer Facilities Management Services	13909
541519	Other Computer Related Services	22346
541618	Other Management Consulting Services	20469
611420	Computer Training	9598
611519	Other Technical and Trade Schools	4043
811212	Computer and Office Machine Repair and Maintenance	5832

The CCR data does not preclude one particular entity from appearing in multiple lines above, so the total number of discrete entities is most likely considerably fewer than the sum of all entities.

Similarly, it is possible to work through the CCR data and extract entities for each PSC of interest. Table A-5 illustrates the number of entries extracted from the CCR data (see Column 3) for a small number of PSC codes most likely to be associated with ICT or cyber technologies.

Table A-5. Number of Entities Listed in the CCR by Selected PSC Codes

PSC Code	PSC Description	# of Entries
4931	Fire Control Maintenance and Repair Shop Specialized Equipment	70
4933	Weapons Maintenance and Repair Shop Specialized Equipment	388
4935	Guided Missile Maintenance, Repair, and Checkout Specialized Equipment	239
5805	Telecommunication Equipment-Nonenvironmental	2897
5810	Communication Security Equipment & Components	4796
5811	Other Cryptologic Equipment & Components	645
5905	Resistors	788
5910	Capacitors	1775
5915	Filters and networks	753
5925	Circuit breakers	1484
5930	Switches	1582
5960	Electron Tubes and Associated Hardware	673
5961	Semi Conductor Devices	1221
5962	Microcircuits	1194
7015	Servers and Mainframes-Nonenvironmental	945
7023	Internal Computer Hardware	351
7025	Computer Accessories	2895
7030	Computer Software	8200
7045	Data Storage Devices	1741
7060	Computer Networking Supplies	546
7080	Computers, PCs and Laptops-Nonenvironmental	792

Summary and Conclusions

We have identified several existing schema that can be used to characterize or describe the current U.S. industrial base and those entities known to be supplying products and services to the DoD based on FPDS reports. The large number of DoD transactions makes extraction of company information from FPDS a challenge, but with diligent searches at the component or subcomponent/contracting office level, we should be able to extract small enough pieces of the database to end up with a useful set of companies that reflect sets of capabilities of interest to DoD. We hypothesize that the number of companies that constitute the gross defense industrial base as represented in the CCR

database will be greater than the number of companies with whom DoD does business directly. Using these data sources, we can begin to work with data that describe a very large fraction of the DoD active and potential industrial base. There are certain exceptions to or limitations on registration and reporting in the FPDS and CCR, but these sources should give us a good handle on instantiation of key attributes of the defense industrial base of concern.

Illustrations

List of Figures

List of Tables

References

Booz-Allen-Hamilton. "Readying the Next Generation Cyber Workforce: Acquiring, Developing and Retaining Cyber Professionals." http://www.boozallen.com/consulting/transform-technology/cybersecurity/cyber-people.

Cavolowsky, John A. "UAS Integration in the NAS Planning Overview." Briefing to the NAC Aeronautics Committee. 23 March 2010. http://www.aeronautics.nasa.gov/pdf/nac_briefing_uas_042310.pdf.

Center for Strategic & International Studies. "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters." A White Paper of the CSIS Commission on Cybersecurity for the 44th Presidency. July 2010. http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity.

Comprehensive National Cybersecurity Initiative (CNCI) #8. 2008. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

Conti, Gregory, and David Raymond. "Leadership of Cyber Warriors: Enduring Principles and New Directions". *Small Wars Journal*. July 2011. http://smallwarsjournal.com/jrnl/art/leadership-of-cyber-warriors-enduring-principles-and-new-directions.

Critical Technology Assessment of the U.S. Semiconductor Materials Industry. Washington, D.C.: Bureau of Industry and Security, U.S. Department of Commerce, April 1977. http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/semiconductormaterialsyr97.html.

Cyber Operations Personnel Report: Report to the Congressional Defense Committees as Required by P.L. 111-84. April 2011.

Defense Strategy for Operations in Cyberspace. July 2011. http://www.defense.gov/home/features/2011/0411_cyberstrategy/.

Deloitte. Cyber Workforce Preparedness Survey Report. 15 October 2010. http://www.deloitte.com/view/en_US/us/Industries/US-federal-government/federal-focus/cyber/8734b2ae4b8ad210VgnVCM1000001a56f00aRCRD.htm.

Department of Defense Cybersecurity Workforce Study. March 2011.

Department of Homeland Security. Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development. September 2008. http://www.us-cert.gov/ITSecurityEBK/.

Executive Office of the President. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. http://www.whitehouse.gov/cyberreview.

Federal CIO Council. *NetGeneration: Preparing for Change in the Federal Information Technology Workforce*. April 2010. http://cio-nii.defense.gov/initiatives/netgenerationguide/index.html.

Frost & Sullivan. *The 2011 (ISC)2 Global Information Security Workforce Study*. https://www.isc2.org/workforcestudy/Default.aspx.

"Global Hawk Update: Diminished Manufacturing Sources." Briefing to Dyke Weatherington and Steve Mozel. March 31, 2009.

Government Accountability Office. "Rare Earth Materials in the Defense Supply Chain." Briefing for Congressional Committees. April 1, 2010. http://www.gao.gov/new.items/d10617r.pdf.

Hoover, J. Nicholas. "Closing the Cybersecurity Skills Gap." http://www.informationweek.com/news/government/security/227100067. http://www.aurora.aero/Common/Images/ResearchDevelopment/RDfact.pdf.

Lee, JinKyu, et al. "Anatomy of the Information Security Workforce." *IEEE IT Pro*. January/February 2010. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5403173&tag=1.

Lynn III, William J., Deputy Secretary of Defense. Remarks on Cyber at the RSA Conference. San Francisco, CA, February 15, 2011.

Office of Management and Budget (OMB). *Fiscal Year 2010 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*. http://www.whitehouse.gov/omb/e-gov/docs/#Recentreportsanddocs.

Office of Personnel Management (OPM). Memorandum for Chief Human Capital Officers, subj: Competency Model for Cybersecurity. 16 February 2011. http://www.chcoc.gov/transmittals/TransmittalDetails.aspx?TransmittalID=3436.

Quadrennial Roles and Missions Report. January 2009. http://www.defense.gov/releases/release.aspx?releaseid=12470.

Rare Earth Materials in the Defense Supply Chain, Briefing for Congressional Committees, GAO. 1 April 2010. http://www.gao.gov/new.items/d10617r.pdf.

Recovering the Domestic Aerospace and Defense Industrial Base. April 2011. National Defense Industrial Association Manufacturing Division – Supply Chain Network Committee. http://www.ndia.org/Divisions/Divisions/Manufacturing/Documents/White%20Papers%202011/NDIA%20White%20Paper-Recovering%20A-D%20Industrial%20Base_FINAL.pdf.

Rockwell, David L. *Military Electronics Briefing Book*. Fairfax, VA: Teal Group, July 2011.

UAV Roundup 2011. Aerospace America. March 2011. http://www.aerospaceamerica.org/Documents/March%202011%20AA%20PDFs/Aerospace%20America%20_MAR2011.pdf.

UND Aerospace. http://uasresearch.com.

Unmanned Aerial Systems: a Challenge to European Industry? K. Hayward. RUSI Defence Systems. June 2010. http://www.rusi.org/downloads/assets/HaywardRDSSummer2010.pdf.

Welch, General Larry D. "Cyberspace—the Fifth Operational Domain." *IDA Research Notes*. Alexandria, VA: Institute for Defense Analyses. Summer 2011.

World Unmanned Aerial Vehicle Systems. *2011 Market Profile and Forecast*. Fairfax, VA: Teal Group.

Abbreviations

ASIC	Application-Specific Integrated Circuit
BAMS	Broad Area Maritime Surveillance
CC	Cubic Centimeter
CCR	Central Contractor Registration
COTS	Commercial Off-the-Shelf
DARPA	Defense Advanced Research Projects Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DMS	Diminishing Manufacturing Sources
DoD	Department of Defense
DRAM	Dynamic Random-Access Memory
EO/IR	Electro-Optical/Infrared
ERU	Electro-Optical Infrared Receiver Unit
EW	Electronic Warfare
FAR	Federal Acquisition Regulation
FMS	Foreign Military Sales
FOIA	Freedom of Information Act
FPA	Focal Plane Array
FPDS	Federal Procurement Data System
FPGA	Field Programmable Gate Array
FSC	Federal Supply Code
FY	Fiscal Year
GA	General Atomics
GAO	General Accountability Office
GCS	Ground Control Station
GD	General Dynamics
GSA	General Services Administration
IARPA	Intelligence Advanced Research Projects Agency
ICT	Information Communication Technology
IDA	Institute for Defense Analyses
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ISR	Intelligence, Surveillance, and Reconnaissance
ITAR	International Traffic in Arms Regulation
JVM	Java Virtual Machine
LM	Lockheed Martin

LOCAAS	Low-Cost Autonomous Attack System
LRIP	Low Rate Initial Production
MALD	Miniature Air-Launched Decoy
MILSPEC	Military Specification
NAICS	North American Industry Classification System
NDIA	National Defense Industrial Association
NG	Northrop Grumman
OEM	Original Equipment Manufacturer
OFPP	Office of Federal Procurement Policy
OMB	Office of Management and Budget
PSC	Product and Service Codes
R&D	Research and Development
RF	Radio Frequency
SμDDL	Secure Micro Digital Data Link
SAR	Synthetic Aperture Radar
SIC	Standard Industrial Classification
SIGINT	Signals Intelligence
TCDL	Tactical Common Data Link
TSMC	Taiwan Semiconductor Manufacturing Company, Limited
U.S.	United States
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
xx-04-2012	Final	May - Nov 2011

4. TITLE AND SUBTITLE
Exploratory Analysis of Supply Chains in the Defense Industrial Base

5a. CONTRACT NUMBER
DASW01-04-C-0003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dominy, James R.
Arnold, Scot A.
Frank, Forrest R.
Holzer, Jenny R.
Richmann, James N.

5d. PROJECT NUMBER

5e. TASK NUMBER
AH-7-3315

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER
IDA Document D-4308

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Deputy Assistant Secretary
of Defense for Manufacturing and Industrial Base Policy
3330 Defense Pentagon, Room 3B854
Washington, DC 20301

10. SPONSOR/MONITOR'S ACRONYM(S)
(Dir, IP)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study used readily available data to perform an exploratory analysis of the supply chains for two sectors of the Defense Industrial Base: unmanned aerial systems, and cyber equipment and services. The results of this study will contribute to a major Department of Defense initiative—the sector-by-sector, tier-by-tier evaluation of the Defense Industrial Base. The study evaluates supply chains in the two sectors to identify segments of the supply chain that depend on sole suppliers or that exhibit constrained competition; interdependencies across program or prime contractors' supplier networks; companies with major capabilities for the design of future products in the sector; the relationship between military and commercial markets; the degree to which the supply chains are global in nature; and the methods by which companies at the various tiers of the supply chain obtain working and investment capital.

15. SUBJECT TERMS
Unmanned Aerial Systems, Cyber, Defense Industrial Base, Supply Chains

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Gholz, Eugene
Unclassified	Unclassified	Unclassified	Same as Report	58	19b. TELEPHONE NUMBER *(Include area code)* (703) 697-0051

Reset